REMARKS

In view of the preceding amendments and the following remarks, the Applicants respectfully request reconsideration of the present application.

Objections and Rejections

The Office Action dated July 16, 2003:

1. objects to the specification;

2. objects to informal drawings;

3. rejects claims 1, 3, 4, 7, 8, 10, 12, 13, 16 and 17 under 35 U.S.C. § 102 as being anticipated by United States Patent no. 4,604,708 entitled "Electronic Security System for Electronically Powered Devices" that issued on August 5, 1986, on a patent application filed by Gainer R. Lewis ("the Lewis patent");

4. rejects claims 6 and 15 under 35 U.S.C. § 103(a) for obviousness based upon the Lewis patent in view of United States Patent no. 5,313,639 entitled "Computer With Security Device for Controlling Access Thereto" which issued May 17, 1994, on a patent application filed by George Chao ("the Chao patent"); and

5. rejects claims 2, 5, 9, 11, 14 and 18 under 35 U.S.C. § 103(a) for obviousness based the Lewis patent in view

-19-

of United States Patent no. 5,594,319 entitled "Battery Pack Having Theft Deterrent Circuit" that issued January 14, 1997, on a patent filed by Iilonga P. Thandiwe ("the Thandiwe patent").

Description of the Amendments

Applicants request amendment of the specification on pages 13 and 15 as set forth above to traverse objections to the specification set forth in the July 16, 2003, Office Action.

Applicants request amendment of the specification on pages 5, 9, 12, and in the Abstract of the Disclosure to insert a "-" into the word "non-volatile."

This Response amends claims 1 and 10 so those claims more particularly point out and distinctly claim the subject matter which the inventors regard as their invention.

The Claimed Invention

The invention, as presently encompassed by independent claim 1, is an integrated circuit pre-boot security controller that includes a non-volatile password memory for storing at least one user password. A password input circuit, included in the pre-boot

-20-

security controller, receives a password for comparison with any user passwords recorded in the password memory. If the pre-boot security controller is in a security operating mode, a digital logic circuit, also included in the pre-boot security controller, compares the received password with any user passwords recorded in the password memory. If the password received by the password input circuit matches a user password recorded in the password memory, an output circuit of the pre-boot security controller, that is coupled to the digital logic circuit, transmits an output signal to a power subsystem to enable energizing operation of a digital computer.

The Cited References

The Lewis patent

The Lewis patent discloses an electronic security system that includes a microcomputer which executes a power-on routine stored in memory whenever the microcomputer is initially coupled to a power source. A user must enter a primary security code (password) which is compared to a predetermined code (user password), and if the codes (password and user password) match, the microcomputer signals a relay to provide power to the device, thereby enabling the device's operation. Once the device is enabled, the user need

not reenter the security code so long as the external source of

power to the device remains uninterrupted.   (Abstract)

> In operation, a device incorporating the present
> invention is supplied with external power, typically by
> coupling line 16 to a household A.C. outlet.   The logic
> power supply 12 converts the A.C. current into a D.C.
> source and provides the requisite D.C. current on line
> 17.   Microcomputer 10, upon the application of power to
> the power supply 12 executes a power-on routine which is
> stored in ROM 32.   The power-on routine, as will be
> described, requires the microcomputer to await the input
> of a code from keypad 24.   **As the user inputs a code,
> microcomputer 10 compares the keyed in security code
> keystroke by keystroke with a predetermined primary
> security code stored in PROM 34.**   If the codes match,
> microcomputer 10 signals the relay driver 18 on line 36
> to provide A.C. power to the device by activating the
> main power relay 22.   Power is thereby provided to the
> device's main power supply 37, or other applicable
> circuit depending on the nature of the device protected.
> Col. 3, lines 41-59.   (Emphasis supplied.)

The Applicant respectfully submits that, for reasons explained

in greater detail below, the electronic security system disclosed

in the Lewis patent at best provides only an illusion of security

if the device disclosed in that reference were stolen as happens

frequently with portable laptop and notebook computers.   Specifi-

cally, if an in-circuit emulator (ICE)[1] were coupled to the

microcomputer 10 disclosed in the Lewis patent, the ICE could be

---

[1]   For example, see United States Patent No. 4,900,014 ("the
'014 patent") that issued May 4, 1999, for a more
complete description of how an ICE may be used to acquire
data that is being accessed by a microprocessor. Copies
of the Abstract and FIG. 2 of the '014 patent are
attached hereto as Exhibit A.

-22-

used to ascertain the "predetermined primary security code stored in PROM 34."

Conversely, the invention encompassed by amended independent claims 1 and 10 locates securely, entirely within a single integrated circuit, both storage for the user password and the digital logic circuit that compares the stored user password with a password received by the integrated circuit. Storing both the user password and the digital logic circuit within a single integrated circuit prevents compromising the user password by any technique other than, perhaps, destroying the integrated circuit.

The Chao patent

The Chao patent discloses a computer having an access control device that includes a casing located in a space in the computer that usually receives one of the computer's disk drives. A password may be entered using a keypad that is located on the front panel of the casing. A control unit included in the casing has a memory which stores a password, and a microprocessor unit which receives the input password from the keypad. If the password received from the keypad matches to password stored in the memory unit, the microprocessor generates an activating signal for at least one control circuit connected to the computer keyboard, the floppy disk drive and/or the main system board. The activating

-23-

signal from the microprocessor unit unlocks and enables the

computer keyboard, the floppy disk drive and/or the main system

board to permit normal operation of the computer.   (Abstract)

The casing (1) has a front panel (10) and a pair of side panels (11, 12) which cooperatively define a receiving space (13). The keypad (2) is provided on the front panel (10) and includes a numeric key set (21) and a function key set (22). The control unit (3) is provided in the receiving space (13) of the casing (1) and is electrically connected to the keypad (2).

The computer (4) has two disk drive receiving spaces (40) . . . . The casing (1) is adapted to be received in one of the disk drive receiving spaces (40).

*   *   *

Referring to FIG. 2, the control unit (3) comprises a microprocessor unit (31), a read only memory (ROM) unit (32), a keyboard control circuit (34), a main system board control circuit (33) and a disk drive control circuit (35).

The ROM unit (32) is preferably an electronic erasable programmable ROM (EEPROM) and is used to store a desired password. The control unit (3) disconnects the output lines of the computer keyboard (42) from the main system board (44) and the floppy disk drive (41) from the computer power supply (43) and maintains the main system board (44) in a reset state in order to prevent the operation of the computer (4) in the absence of a correct input password.

The keypad (2) is operated so as to provide an input password to the microprocessor unit (31). The microprocessor unit (31) then compares the input password with the desired password which has been previously stored in the ROM unit (32). If both passwords tally, the microprocessor unit (31) generates a high logic signal at the control lines (P1, P2, P3). The control lines (P1, P2, P3) are connected to the switching transistor (Q33, Q34, Q35) of a respective one of the control circuits (33, 34, 35). Each of the control circuits (33, 34, 35) further comprises a relay unit (331, 341, 351) which has a coil (L33, L34, L35) connected to the respective switching transistor (Q33, Q34, Q35). A high logic signal at the control lines (P1, P2, P3) causes the switching transistors (Q33, Q34, Q35) to conduct, thereby energizing the

-24-

coils (L33, L34, L35) to connect the disk drive (41) to the power supply (43), to connect the output lines of the keyboard (42), and the main system board (44), and to disconnect a power on reset circuit (441) of the main system board (44) from a clock generator circuit (442) of the same. This permits normal operation of the computer (4). Col. 2, line 34 - col. 3, line 14. (Emphasis supplied.)

It is clear from the preceding excerpt quoted from the Chao patent that the reference's access control device provides no more real security than the electronic security system disclosed in the Lewis patent. In fact the access control device disclosed in the Chao patent appears to provide less security than that provided by the Lewis patent's electronic security system. For example, the casing (1) can be easily removed from the disk drive receiving space (40) and replaced by an identical substitute casing which holds a known password in the replacement casing's ROM unit (32). Another way to defeat the apparent security provided by the Chao patent's casing (1) is to merely remove it and substitute jumpers for the relay unit (331, 341, 351) thereby entirely eliminating any need for entry of a password.

Conversely, the invention encompassed by amended independent claims 1 and 10 locates securely, entirely within a single integrated circuit, both storage for the user password and the digital logic circuit that compares the stored user password with a password received by the integrated circuit. Storing both the user password and the digital logic circuit within a single

-25-

integrated circuit prevents compromising the user password by any
technique other than, perhaps, destroying the integrated circuit.

The Thandiwe patent

The Thandiwe patent discloses a battery pack (10) includes a
memory (26) for storing a password. Upon connecting the battery
pack (10) to a host device (12), the battery waits for a data word
to be communicated from the host device over a communications
channel (22). If an incorrect data word is received a predeter-
mined number of time, or if an initial power time period, as
defined by a timer (30), elapses, a switch (16) is opened, thereby
disconnecting the battery cell or cells (14) from the load.
(Abstract)

> The battery cell or cells, along with the associated
> interconnection circuitry, and electronic circuits
> described herein are housed in a battery pack housing .
> . . . A switch 16 is coupled in series with the battery
> cell or cells, and is operable in either a closed,
> conductive state, and an open, non-conductive state.
>   *   *   *
> The switch is also connected to a control circuit, such
> as, preferably, a microcontroller circuit 20, and is
> responsive to a signal provided by the control circuit.
>   *   *   *
> In operation, the battery pack, once connected to
> the host device, receives a data word from the host
> device over a communications channel 22 . . . .
>   *   *   *
> A communications circuit 24 in the battery pack, and part
> of the microcontroller circuit [20], receives the data
> word over the channel 22. The data word is compared to
> a password stored in a memory 26 by some means for
> comparing, such as a logic circuit 28, which is also part

-26-

of the microcontroller circuit. Upon a predetermined
number of occurrences of the data word differing from the
password, a means for controlling the switch, which may
also be the logic circuit, will open the switch 16.

       *   *   *

The battery pack then prompts the host device to send a
data word, and in turn, the host device prompts the user
to enter a data word. The host device then communicates
the entered data word to the battery pack. If the data
word does not match the password, the battery pack may
signal the host device, which in turn prompts the user
again. This continues until either the user enters the
correct data word, or the battery pack disables itself.
Col. 2, lines 1-55.

First, Applicants observe that the Thandiwe patent operates in

a manner diametrically opposite to that disclosed and claimed in

the present invention. That is, the battery pack 10 fully powers

the operation of the host device 12 throughout a data word (pass-

word) entry time interval until either:

1.   incorrect data words (passwords) are received a predeter-

       mined number of times; or

2.   the data word (password) entry time interval elapses.

During the interval throughout which the battery pack 10 awaits the

arrival of the data word (password) from the host device 12, the

host device 12 appears to be fully operational for any purpose.

Conversely, the present application discloses and claims withhold-

ing power from everything but the pre-boot security controller

integrated circuit until a user enters the correct password.

Second, the invention disclosed in the Thandiwe patent

provides no more true security than that described in the Chao

-27-

patent. That is, in a manner analogous to that described above for the Chao patent, the secure battery system described in the Thandiwe patent can be avoided merely by connecting to the host device 12 a substitute battery pack (10) having a known password stored in its memory 26. Alternatively, a battery pack entirely lacking the microcontroller circuit 20 and the logic circuit 28 can be connected to the host device 12 for energizing its operation without any need to enter a password.

Conversely, the invention encompassed by amended independent claims 1 and 10 locates securely, entirely within a single integrated circuit, both storage for the user password and the digital logic circuit that compares the stored user password with a password received by the integrated circuit. Storing both the user password and the digital logic circuit within a single integrated circuit prevents compromising the user password by any technique other than, perhaps, destroying the integrated circuit.

Argument

Applicants respectfully submit that amended independent claims 1 and 10 traverse rejection under 35 U.S.C. § 102(b) based upon the Lewis patent first because the present application discloses an operation which is diametrically opposite to that disclosed in the Lewis patent. That is, the present application discloses that the

-28-

digital computer remains un-energized until after entry of the correct password. Conversely, the Lewis patent discloses fully energizing the microcomputer 10 throughout a password entry time interval. Second, the Lewis patent discloses that the microprocessor 10 compares a password entered by a user with one stored in the PROM 34. As described above, connecting an ICE to the microcomputer 10 while entering an incorrect password permits ascertaining the password stored in the PROM 34.

Thus, because the Lewis patent doesn't disclose, either expressly or inherently, the present invention as embodied in independent claims 1 and 10, Applicants respectfully submit that those claims traverse rejection under 35 U.S.C. § 102(b).

Moreover, because independent claims 1 and 10 traverse rejection under 35 U.S.C. § 102(b), Applicants respectfully submit that claims 2-9 and 11-18, which respectively depend either directly or indirectly from independent claims 1 and 10, also traverse the rejections set forth in the July 16, 2003, Office Action both:

1. under 35 U.S.C. § 102(b) based solely upon the Lewis patent; or

2. under 35 U.S.C. § 103(a) based upon the Lewis patent in view of either the Chao or Thandiwe patents.

-29-

Conclusion

Since the Applicants will furnish formal drawings when there are allowed claims and have amended the specification to traverse the objections set forth in the July 16, 2003, Office Action, Applicants respectfully request consideration of the amended claims.

For the reasons set forth above, independent claims 1 and 10 traverse rejection under 35 U.S.C. § 102(b) based upon the Lewis patent, and claims 2-9 and 11-18 traverse rejection both:

1. under 35 U.S.C. § 102(b) based solely upon the Lewis patent; or

2. under 35 U.S.C. § 103(a) based upon the Lewis patent in view of either the Chao or Thandiwe patents.
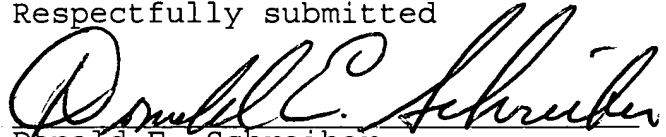
///

///

///

///

///

///

///

///

For the preceding reasons, Applicants respectfully request that all objections and rejections be withdrawn, and this patent application pass to issue.

Respectfully submitted

Donald E. Schreiber
Reg. No. 29,435

Dated: *14 October*, 2003

Donald E. Schreiber
A Professional Corporation
Post Office Box 2926
Kings Beach, CA 96143-2926

Telephone: (530) 546-6041

Attorney for Applicants

-31-

US005900014A

United States Patent [19]

Bennett

[11] **Patent Number:** **5,900,014**

[45] **Date of Patent:** **May 4, 1999**

[54] **EXTERNAL MEANS OF OVERRIDING AND CONTROLLING CACHEABILITY ATTRIBUTE OF SELECTED CPU ACCESSES TO MONITOR INSTRUCTION AND DATA STREAMS**

[75] Inventor: **Brian R. Bennett**, Laguna Niguel, Calif.

[73] Assignee: **AST Research, Inc.**, Irvine, Calif.

[21] Appl. No.: **08/769,321**

[22] Filed: **Dec. 19, 1996**

Related U.S. Application Data

[63] Continuation of application No. 08/351,759, Dec. 8, 1994, abandoned.

[51] **Int. Cl.**[6] **G06F 12/08**; G06F 11/30
[52] **U.S. Cl.** **711/138**; 395/183.05; 395/183.14; 395/183.15; 395/704; 395/568
[58] **Field of Search** 711/138, 139, 711/121, 122; 395/183.15, 183.14, 185.05, 185.06, 185.09, 704, 568, 183.04, 183.05

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,758,946	7/1988	Shar et al.	711/206
4,885,680	12/1989	Anthony et al.	711/144
5,075,846	12/1991	Reininger et al.	364/400
5,249,281	9/1993	Fuccio et al.	711/123
5,325,499	6/1994	Kummer et al.	711/133
5,327,545	7/1994	Begun et al.	711/143
5,355,467	10/1994	MacWilliams et al.	711/146
5,404,464	4/1995	Bennett	395/281
5,463,760	10/1995	Hamauchi	711/3
5,619,677	4/1997	Nishimukai et al.	711/138
5,636,363	6/1997	Bourekas et al.	711/138

FOREIGN PATENT DOCUMENTS

64-002155 1/1989 Japan .

OTHER PUBLICATIONS

Atmel Travels New Worlds, Electronic Buyers' News Mar. 14, 1994, p.14.

Case Brian, ARM600 targets low–power applications: ARM core extended with 32–bit addressing, "object oriented" MMU, Microprocessor Report, v5, n23, p8(4), Dec. 18, 1991.

Gallant, Protocols keep data consistent; cache–coherency protocols, EDN, v36, n6, p41(6), Mar. 14, 1991.

Shear, David; Teaming a Logic Analyzer with a Debugger Provides Advantages to Both Tools, EDN–Technology Update, Jan. 20, 1994 pp. 21–26.
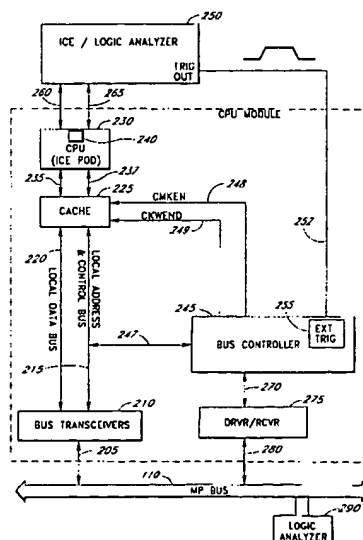
Primary Examiner—Eddie P. Chan
Assistant Examiner—Reginald G. Bragdon
Attorney, Agent, or Firm—Knobbe, Martens, Olson & Bear, LLP

[57] **ABSTRACT**

A system for facilitating debugging of software running within an information processing unit includes an external trigger state machine which selectively overrides the cacheability attribute of a cache line. An in-circuit emulator (ICE), which is used for debugging purposes, monitors addresses read by and written to a CPU. If an address which is of interest for debugging purposes is detected by the ICE, then the ICE issues a trigger signal. The trigger signal causes the external trigger state machine to designate the cache line associated with the detected address as a non-cacheable operation (i.e., to override the cacheability attribute) . Thus, the data associated with the cache line is written out to the main memory module where the data can be observed by an ICE, rather than to an internal cache memory location where the data would be invisible to an ICE. In a preferred embodiment of the invention, the external trigger state machine is configured to operate in a pipelining environment wherein multiple requests may be outstanding at one time.
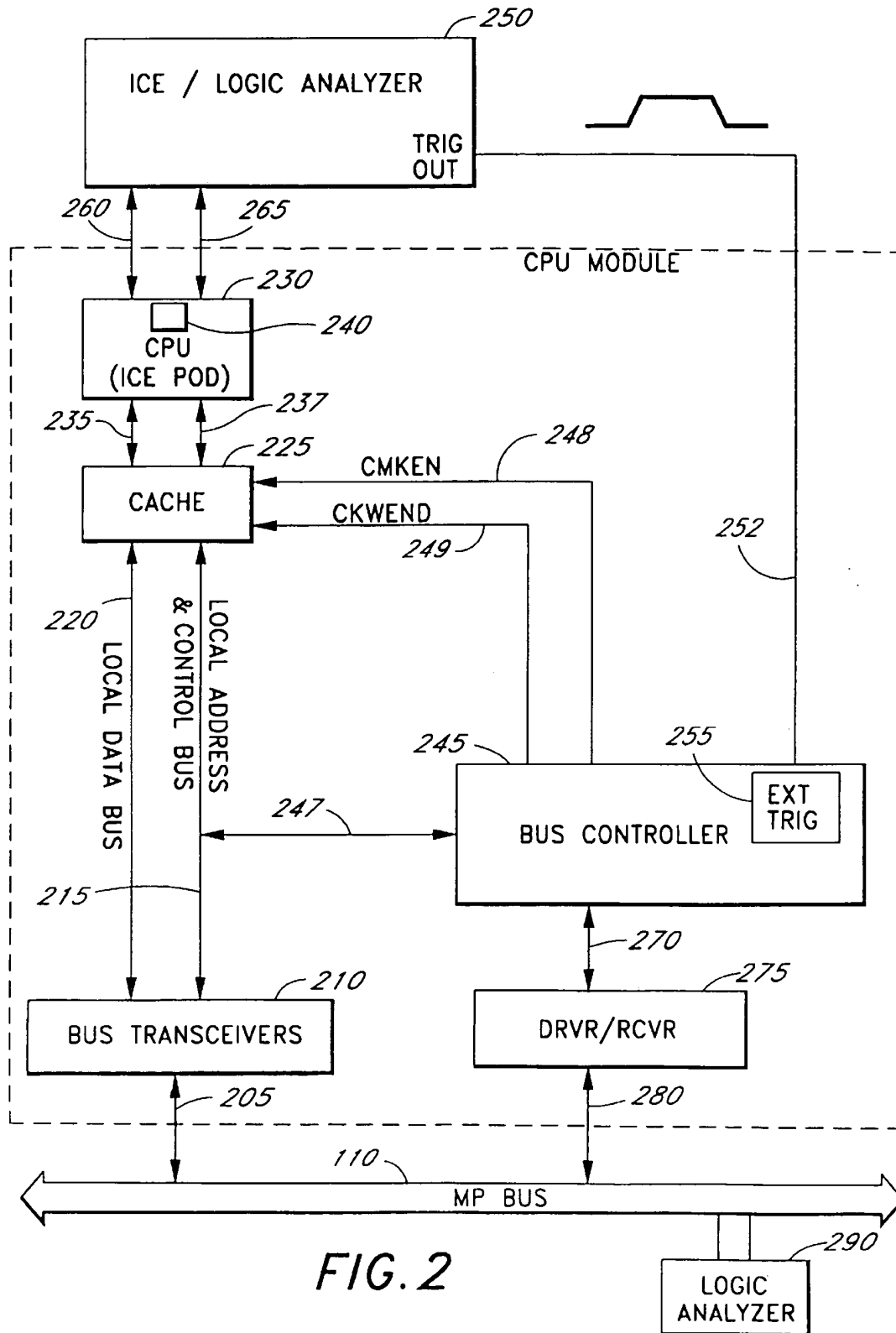
8 Claims, 4 Drawing Sheets

FIG.2